

***SECURITY: attività professionale volta prevenire fronteggiare e superare eventi originati da azioni in prevalenza illecite che espongono le persone, i beni e le strutture a potenziali effetti lesivi o dannosi.
Illecito non è solo il comportamento antigiuridico ma anche quello in contrasto con le procedure interne dell'Organizzazione.***

**SERVIZI RIVOLTI ALLE ORGANIZZAZIONI
Focus particolare: uffici ed attività all'estero.**

1. Formazione individuale.

 è un programma di consulenza e formazione finalizzato ad accrescere le capacità in tema di *security*.

 prevede moduli alternativi di intensità differente e composti da lezioni individuali i cui orari e contenuti sono scelti dalla persona interessata.

2. Supporto a distanza.

 prevede supporto individuale a distanza attivabile in ogni momento. Il supporto a distanza viene programmato sulle esigenze del contingenti e fornisce informazioni ed appoggio agli operatori in tema di *security*.

3. Formazione per gruppi ed organizzazioni.

In base alle esigenze emergenti in un gruppo o all'interno di un'Organizzazione, si realizzano percorsi formativi *ad hoc* in tema di *security*

4. Consulenza.

Gli argomenti oggetto di affiancamento sono:

- gestione integrata del rischio in relazione agli standard della serie UNI ISO 31000.
- Controllo degli impatti fonte di interruzioni operative. UNI EN ISO 22301:2019.
- *Security* dell'organizzazione. Norma di riferimento UNI 10459:2022.
- Conformità al Dlgs. 231/2001: responsabilità da reato degli enti.
- Leggi e standard sulla protezione di informazioni aziendali e dati personali.

Protezione di beni e strutture.

- Analisi dello scenario, del contesto esterno ed interno.
- Elaborazione e attuazione piano di security.
- Elaborazione della struttura organizzativa e del budget di funzione.
- Antifrode.
- Antintrusione.
- Conformità a prescrizioni legali ed altre prescrizioni afferenti la security.
- Coordinamento dei sistemi integrati di sicurezza delle strutture.
- Coordinamento della piano Continuità Operativa e Disaster Recovery.
- Gestione della vigilanza privata e dei servizi di sicurezza privati.
- Gestione delle crisi (Crisis Management).
- Gestione della protezione delle informazioni, incluso il coordinamento e supporto alle attività relative alla sicurezza delle informazioni.
- Business/competitive intelligence.
- Audit tecnico di security.
- Monitoraggio e relazione di security.
- Tutela del know-how, segreto industriale e delle risorse immateriali.
- Protezione da spionaggio industriale.
- Protezione di infrastrutture critiche.
- Supervisione della gestione di contratti afferenti alla security.

Protezione delle persone.

- Analisi dei rischi di security sulla persona.
- Gestione dei rischi di security.
- Supporto al datore di lavoro a tutela dei lavoratori da rischi di origine criminosa.
- Attività formativa/informativa al personale sui rischi di security.
- Gestione e coordinamento delle risorse umane ed economiche di security
- Gestione delle investigazioni private affidate a terzi.
- Protezione e tutela del management dell'Organizzazione.
- Rapporti con le Forze di Polizia e Forze armate, agenzie e istituzioni pubbliche.